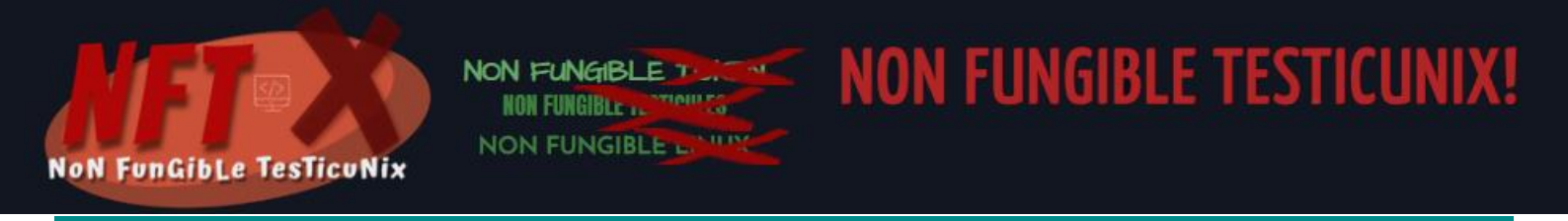

Toujours trés utile, voir indispensable si vous bidouillez sur des serveurs, des machines virtuelles, sur un lan à la maison...
Attardons nous un instant sur ce protocole, je vous propose ici un installation toute basique sur un Ubuntu 20.04.

SSH est un protocole permettant d'établir une communication chiffrée, donc sécurisée (on parle parfois de tunnel), sur un réseau informatique (intranet ou Internet) entre une machine locale (le client) et une machine distante (le serveur).

La sécurité du chiffrement peut être assurée par différentes méthodes, entre autres par mot de passe ou par un système de clés publique / privée (mieux sécurisé, on parle alors de cryptographie asymétrique).

Nous devons tout d'abord installer ssh-serveur sur notre machine, ssh-client est normalement installé par défaut sur les systèmes Ubuntu. Vous pouvez aussi taper ssh -V pour voir si il est déjà installé et voir la version.

Comme d'hab ouvrez un terminal (Ctrl+t sous Ubuntu) et taper les commandes suivantes :

```
#pour commencer et ça fait pas de mal on fait un petit

sudo apt update && apt upgrade -y

#ensuite on installe notre serveur SSH

sudo apt install openssh-server

#et on démarre le service

sudo systemctl start ssh
```

Voila c'est pas plus compliqué...

On va maintenant éditer le fichier de config et autoriser la connexion en root

```
sudo nano /etc/ssh/sshd_config

#Dans le fichier on fait Ctrl+w pour rechercher la ligne PermitRootLogin et on ecrit yes à la fin:

PermitRootLogin yes
```

La manip est à reproduire sur les postes sur lesquels on va vouloir se connecter.

Le système de clé privée/clé publique est bien pratique avec SSH, ça permet par exemple de pas être obligé de taper son mdp à chaque fois qu'on veut se connecter à notre machine distante...

Pour se faire nous allons devoir générer la clé sur notre poste de travail:

```
ssh-keygen -t rsa
```

La passphrase n'est pas obligatoire mais quand même recommandée...sinon appuyez Entrée jusqu'à la fin...

Votre clé est générée, elle se trouve dans le dossier caché ~/.ssh/id_rsa.pub, il faut maintenant l'envoyer sur le poste auquel vous voulez établir la connexion SSH

```
#utilisez simplement
ssh-copy-id <username>@<ipaddress>

#ou

ssh-copy-id -i ~/.ssh/id_rsa.pub <username>@<ipaddress>
```

Voila, si je veux me connecter en root à l'ordi nomé toto, je tape :

```
ssh root@toto
```

Et hop je suis connecté sur toto, même pas besoin de taper de mdp grace à la clé publique!